APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,996	07/07/2003	Tommy Olaus Johnson	19903.0043	9812

23517   7590   12/28/2007
BINGHAM MCCUTCHEN LLP
2020 K Street, N.W.
Intellectual Property Department
WASHINGTON, DC 20006

EXAMINER
GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
12/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/612,996	JOHNSON ET AL.
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/1/07*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-30,32-50,52-60 and 62-64* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-30,32-50,52-60 and 62-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   A request for continued examination under 37 CFR 1.114, including the

fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection.

Since this application is eligible for continued examination under 37 CFR 1.114,

and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the

previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Applicant's submission filed on October 1, 2007 has been entered.

2.   Claims 1-10, 12-30, 32-50, 52-60, and 62-64 are pending.

Response to Arguments

3.   Applicant's arguments filed October 1, 2007 have been fully considered

but some of the applicant's arguments are not persuasive. The rest of Applicant's

arguments have been considered but are moot in view of the new ground(s) of

rejection. In response to the applicant's argument the following comments are

made:

4.   The applicant argued that Tso fails to meet applicant's claimed "receiving

a request from the computer malware scanning software for data comprising a

randomly accessed portion of the requested file", as specially claimed. The

examiner disagrees. Tso teaches a virus checker may be implemented as a

software module installed on network device or on a separate device coupled to

network device. Virus checking is implemented in a manner intended to

maximize efficient transfer of data from server to client device. Content server will

transmit a requested data object as a series of contiguous portions. Virus

checker performs virus checking on the requested file as portions are received

from content server. (col.2, line 38-col. 3, line 54) Applicant specification on page

4, line 18-page 5, line 2 teaches that "The requested portion of the requested file

may not be transferred because the requested portion of the requested file

cannot be randomly accessed. An indication that the requested portion of the

requested file cannot be randomly accessed may comprise an error indication or

a transfer of the entire requested file." Claims are to be given their broadest

interpretation in light of the specification, the examiner has interpreted from the

above teaching that "randomly accessed portion of the requested file" can

comprise any message other than an error indication or transfer of an entire

requested file. Therefore, Tso teaches receiving a request form the malware

scanning software for data comprising randomly accessed portion of the

requested file. (i.e. a requested data object as a series of contiguous portions)

Tso further teaches objects in cache storage may include a virus checking status

indicator and a pattern version number ... then when a request for a cached

object is received, virus checker need only check the parts of the virus pattern file

that have changed since the data object was cached. Tso further teaches

retrieving a data object to be downloaded to the client, scanning the data object

for a computer virus and downloading the data object to the client if no computer

virus is detected, wherein the data object is segmented into a series of

contiguous portions, retrieving, scanning and downloading steps being performed

for each of said contiguous portions. (col. 5, lines 27-42; col. 9, lines 1-8)

The applicant further argued that Fielding reference does not specifically teach a technique "wherein the randomly accessed portion of the file is requested utilizing a byte range technique". The examiner disagrees. Fielding teaches if a client has a partial copy of an entity in its cache (i.e. randomly accessed portion of a file), and wishes to up-to-date copy of the entire entity in its cache, it could use range request (i.e. byte range) with a conditional GET. (page 82, 14.27 If-Range)

The applicant argued that that prior art cited does not teach "tracking information associated with each transfer of a requested portion of the file". Tso teaches cache storage may include a virus checking status indicator and a pattern version number ... then when a request for a cached object is received, virus checker need only check the parts of the virus pattern file that have changed since the data object was cached. (col. 5, lines 27-42) Fielding also teaches if the client has no entity tag for an entity, but does not have last modified date, it may use the date in If-range header. Checking entity tag and modified date is adequate to meet the claimed limitation (i.e. tracking information)

5.   The applicant argued that prior art does not teach a technique "wherein the byte range technique turns a serial download mechanism into a random access file mechanism". The examiner would like to point out claims are to be given their broadest reasonable interpretation in light of the supporting disclosure. Accordingly, defined in the dictionary "serial means arranged in a series" and "random means having no specific pattern (any order)". Fielding teaches a client that has one or more entities previously obtained from the

resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. The purpose of this feature is to allow efficient updates of cached information with a minimum amount of transaction overhead. It is also used, on updating requests, to prevent inadvertent modification of the wrong version of a resource. If any of the entity tags match the entity tag of the entity that would have been returned in the response to a similar GET request (without the If-Match header) on that resource, or if"*" is given and any current entity exists for that resource, then the server MAY perform the requested method as if the If-Match header field did not exist. A server MUST use the strong comparison function to compare the entity tags in If-Match. If none of the entity tags match, or if"*" is given and no current entity exists, the server MUST NOT perform the requested method, and MUST return a 412 (Precondition Failed) response. The If-Modified-Since request-header field is used with a method to make it conditional: if the requested variant has not been modified since the time specified in this field, an entity will not be returned from the server; instead, a 304 (not modified) response will be returned without any message-body. If-Modified-Since = "If-Modified-Since ...." HTTP-date. If the variant has been modified since the If-Modified- Since date, the response is exactly the same as for a normal GET. (page 80; 14.24 and 14.25)

6.   Fielding further teaches if a client has a partial copy of an entity in its cache, and wishes to have an up-to-date copy of the entire entity in its cache, it could use the Range request-header with a conditional GET (using either or both of If-Unmodified-Since and If-Match.) However, if the condition fails because the

entity has been modified, the client would then have to make a second request to obtain the entire current entity-body. The If-Range header allows a client to "short-circuit" the second request. Informally, its meaning is 'if the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity. (page 82, If-Range)

7.   The applicant argued that the prior art is also deficient with "determining that the requested portion of the requested file cannot be transferred; and transferring an entirety of the requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file" and "wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed." Fielding teaches a client that has one or more entities previously obtained from the resource can verify that one of those entities is current by including a list of their associated entity tags in the If-Match header field. The purpose of this feature is to allow efficient updates of cached information with a minimum amount of transaction overhead. It is also used, on updating requests, to prevent inadvertent modification of the wrong version of a resource. If any of the entity tags match the entity tag of the entity that would have been returned in the response to a similar GET request (without the If-Match header) on that resource, or if"*" is given and any current entity exists for that resource, then the server MAY perform the requested method as if the If-Match header field did not exist. A server MUST use the strong comparison function to compare the entity tags in If-Match. If none of the entity tags match, or

if"*" is given and no current entity exists, the server MUST NOT perform the

requested method, and MUST return a 412 (Precondition Failed) response. The

If-Modified-Since request-header field is used with a method to make it

conditional: if the requested variant has not been modified since the time

specified in this field, an entity will not be returned from the server; instead, a 304

(not modified) response will be returned without any message-body. If-Modified-

Since = "If-Modified-Since ...." HTTP-date. If the variant has been modified since

the If-Modified- Since date, the response is exactly the same as for a normal

GET. The If-Range header allows a client to "short-circuit" the second request.

Informally, its meaning is 'if the entity is unchanged, send me the part(s) that I am

missing; otherwise, send me the entire new entity. (page 80; 14.24 and 14.25;

page 82, If-Range)

In response to applicant's arguments against the references individually,

one cannot show nonobviousness by attacking references individually where the

rejections are based on combinations of references. See *In re Keller*, 642

F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231

USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 101

8.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or
> composition of matter, or any new and useful improvement thereof, may obtain a patent
> therefor, subject to the conditions and requirements of this title.

9.   Claims 1, 21 and 41 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1, 21 and 41 are directed to scanning a requested file for a computer malware, the claimed subject matter relates only to transferring the requested portion of a file, supplying the requested data to the computer malware scanning software and determining whether information associated with the file has changed without performing any scanning a requested file for a computer malware.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1-10, 12-30, 32-50, 52-60, and 62-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tso et al. (hereinafter Tso) US Patent 6,088,803 in view of Fielding et al. "Hypertext Transfer Protocol -- HTTP/1.1", RFC, June 1999, (hereinafter Fielding).

As per claims 1, 21 and 41

Tso teaches a method of scanning a requested file for a computer malware comprising the steps of:

receiving a request to transfer a file from computer malware scanning

software; (col. 2, lines 16-67)

receiving a request from the computer malware scanning software for data

comprising a randomly accessed portion of the requested file; (col. 3, lines 10-54;

col. 5, lines 1-43) and

transferring the requested portion of the file and supplying the requested

data to the computer malware scanning software to fulfill the request for data

comprising a portion of the requested file; (col. 3, lines 10-54; col. 5, lines 1-43)

Tso does not explicitly disclose wherein the randomly accessed portion of

the file is requested utilizing a byte range technique; tracking information with

each transfer of a requested portion of the file; and determining whether the file

has changed; wherein the byte range technique turns a serial download

mechanism into a random access file mechnism. Fielding in analogous art,

however discloses wherein the randomly accessed portion of the file is requested

utilizing a byte range technique; tracking information with each transfer of a

requested portion of the file; and determining whether the file has changed;

wherein the byte range technique turns a serial download mechanism into a

random access file mechnism. (page 80; 14.24 and 14.25; pages 82-83, Section

14.27: If-Range; Pages 85-86, Section 14.35 Range) Therefore it would have

been obvious to one ordinary skill in the art at the time the invention was made to

modify the device disclosed by Tso with Fielding in order to request one or more

sub-ranges of a file, instead of the entire file, using the range request header to

have an up-to-date copy of the entire file. (page 82, 14.27 If-Range; Fielding)

As per claims 2, 22 and 42:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Tso further discloses a method wherein the request

to transfer the file from the computer malware scanning software comprises a

request to transfer the file from an external system. (col. 2, lines 22-25)

As per claims 3-4, 23-24 and 43-44:

The combination of teaches all the subject matter as discussed above. In

addition, Tso further discloses a method wherein the external system is

communicatively connected via a network. (figure 1)

As per claims 5, 18, 25, 38, 45 and 58:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Fielding further discloses a method wherein the

step of transferring the requested portion of the file comprises the step of:

initiating a session with the external system to obtain the requested portion of the

file. (pages 82-83, Section 14.27: If-Range; Pages 85-86, Section 14.35 Range)

As per claims 6, 19, 26, 39, 46 and 59:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Fielding further discloses a method wherein the

session is a hypertext transfer protocol session. (pages 82-83, Section 14.27: If-

Range; Pages 85-86, Section 14.35 Range)

As per claims 15, 35 and 55:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Tso further discloses a method comprising the step

of: performing the steps of claim 1 in response to a request from a user system

for the file. (col. 2, lines 16-67)

As per claims 16, 36 and 56:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Tso further discloses a method comprising the

steps of: scanning at the computer malware scanning software the data

comprising a portion of the requested file to determine if the file includes a

computer malware; (col. 3, lines 10-54) and delivering the file to the user system

in response to determining that the file does not include a computer malware.

(col. 3, lines 38-65)

As per claims 17, 37 and 57:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Fielding further discloses a method wherein the

step of delivering the file to the user system comprises the steps of: determining

whether the entire file has been transferred; (pages 82-83, Section 14.27: If-

Range; Pages 85-86, Section 14.35 Range) starting delivery of the file to the

user system even if the entire file has not been transferred; (pages 82-83,

Section 14.27: If-Range; Pages 85-86, Section 14.35 Range) and transferring

those portions of the file that have not been transferred and delivering those

portions of the file once they have been transferred. (pages 82-83, Section 14.27:

If-Range; Pages 85-86, Section 14.35 Range)

As per claims 7, 20, 27, 40, 47 and 60:

The combination of Tso and Fielding teaches all the subject matter as discussed above. In addition, Fielding further discloses wherein the hypertext transfer protocol session uses the byte range technique. (pages 82-83, Section 14.27: If-Range; Pages 85-86, Section 14.35 Range)

As per claims 8, 28 and 48:

The combination of Tso and Fielding teaches all the subject matter as discussed above. In addition, Fielding further discloses a method comprising the steps of: determining that the requested portion of the requested file cannot be transferred; (pages 82-83, Section 14.27: If-Range; Pages 85-86, Section 14.35 Range) and transferring an entirety of the requested file and supplying the requested data to the computer malware scanning software to fulfill the request for data comprising a portion of the requested file. (pages 82-83, Section 14.27: If-Range; Pages 85-86, Section 14.35 Range)

As per claims 9, 29 and 49:

The combination of Tso and Fielding teaches all the subject matter as discussed above. In addition, Fielding further discloses a method wherein the requested portion of the requested file cannot be transferred because the requested portion of the requested file cannot be randomly accessed. (pages 82-83, Section 14.27: If-Range; Pages 85-86, Section 14.35 Range)

As per claims 10, 30 and 50:

The combination of Tso and Fielding teaches all the subject matter as discussed above. In addition, Fielding further discloses a method wherein an indication that the requested portion of the requested file cannot be randomly

accessed comprises an error indication or a transfer of the entire requested file.

(pages 82-83, Section 14.27: If-Range; Pages 85-86, Section 14.35 Range)

As per claims 12, 32 and 52

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Fielding further discloses a method wherein the

information comprises hypertext transfer protocol entity tags or last modified

timestamp information. (pages 82-83, Section 14.27: If-Range; Pages 85-86,

Section 14.35 Range)

As per claims 13, 33 and 53:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Tso further teaches a method comprising the step

of: restarting the requests from the computer malware scanning software for

data. (col. 3, lines 10-54)

As per claims 14, 34 and 54:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Fielding further discloses a method comprising the

step of: transferring an entirety of the requested file. (pages 82-83, Section

14.27: If-Range; Pages 85-86, Section 14.35 Range)

As per claim 62:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Tso further teaches a method wherein the data

associated with the request from the computer malware scanning software

comprises a plurality of selected randomly accessed portions of the requested

file. (col. 3, lines 10-54; col. 5, lines 1-43)

As per claim 63:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. In addition, Tso further teaches a method wherein the plurality

of randomly accessed portions of the requested file are read in a random order.

(col. 3, lines 10-54; col. 5, lines 1-43)

3.   Claims 64 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Tso et al. (hereinafter Tso) US Patent 6,088,803 in view of Fielding et al.

"Hypertext Transfer Protocol -- HTTP/1.1" (hereinafter Fielding) and further in

view of Ji et al. (hereinafter Ji) U.S. Patent Number 6,728,886.

As per claim 64:

The combination of Tso and Fielding teaches all the subject matter as

discussed above. Both references do not explicitly disclose a method wherein a

system call handler intercepts system level calls made by the computer malware

scanning software and simulates system level function calls utilized by the

computer malware scanning software to determine whether the file includes the

computer malware. Ji in analogous art, however, discloses a system call handler

intercepts system level calls made by the computer malware scanning software

and simulates system level function calls utilized by the computer malware

scanning software to determine whether the file includes the computer malware.

(col. 6, line 5-col. 8, line 10) Therefore it would have been obvious to one

ordinary skill in the art at the time the invention was made to modify the device

disclosed by Tso and Fielding with Ji Guthrie in order to provide additional

security by intercepting http messages enabling browser with additional

functionality without modifying the browser. (page 82, 14.27 If-Range; Fielding)

Any inquiry concerning this communication or earlier communications from

the examiner should be directed to Shewaye Gelagay whose telephone number

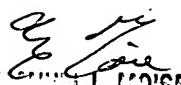is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The

fax phone number for the organization where this application or proceeding is

assigned is 571-273-8300.

Information regarding the status of an application may be obtained from

the Patent Application Information Retrieval (PAIR) system. Status information

for published applications may be obtained from either Private PAIR or Public

PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free). If you would like assistance from a USPTO Customer Service

Representative or access to the automated information system, call 800-786-

9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay

FREDERICK L. MOISE
SUPERVISORY PATENT EXAMINER